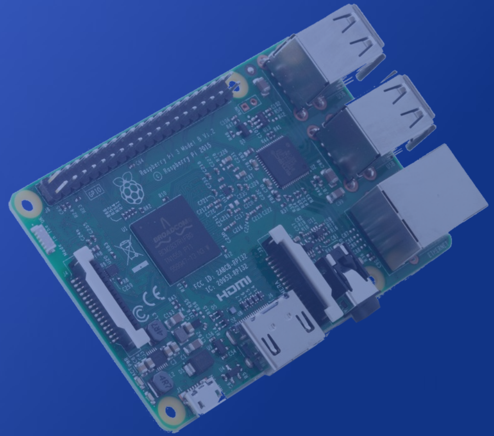
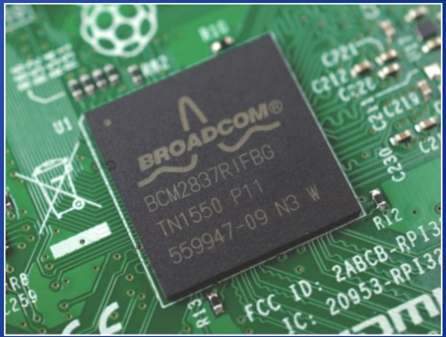
Machine Learning
&
Single Board Computer



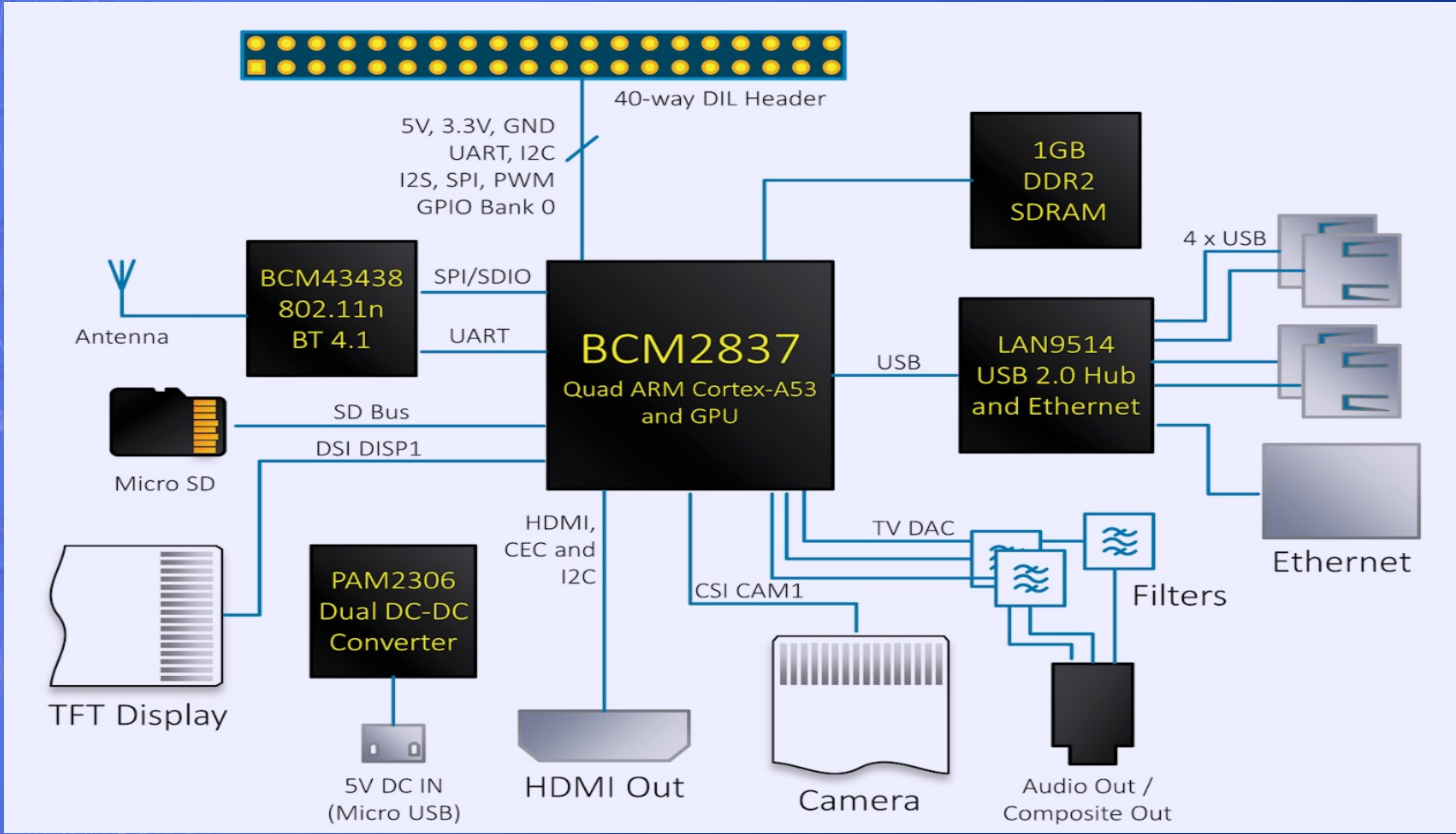
costruire un rilevatore di cyber attack con Raspberry PI

Il panorama delle SBC per il Machine Learning



- Capacità di calcolo elevate preferibilmente con uso di GPU/TPU
- Possibilità di utilizzo di librerie e tool per lo sviluppo rapido
- Interfacce ad alto livello
- Sistemi di comunicazione ad alta velocità (Ethernet, USB, CSI, ecc)
- Stabilità termica

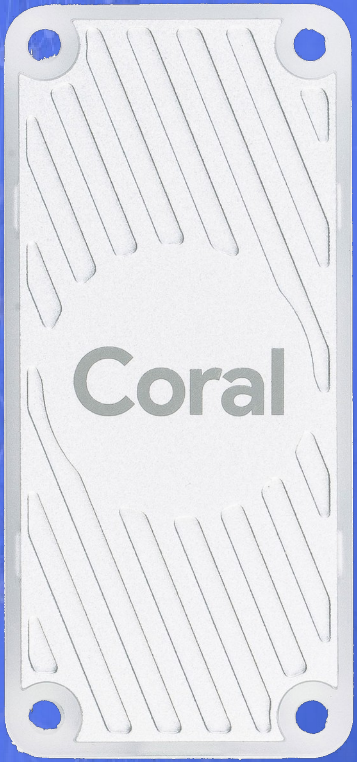
System on Chip



Machine Learning on site
La corsa dei Big Player

- Inizio lento, sviluppo dedicato
- Supporto per TF
- Supporto per Raspberry Pi
- Costo sostenibile inferiore a 100$
- Nvidia Jatson e Google Coral

Google Coral TPU



Coral & Raspberry pi 3

Sono compatibili ?

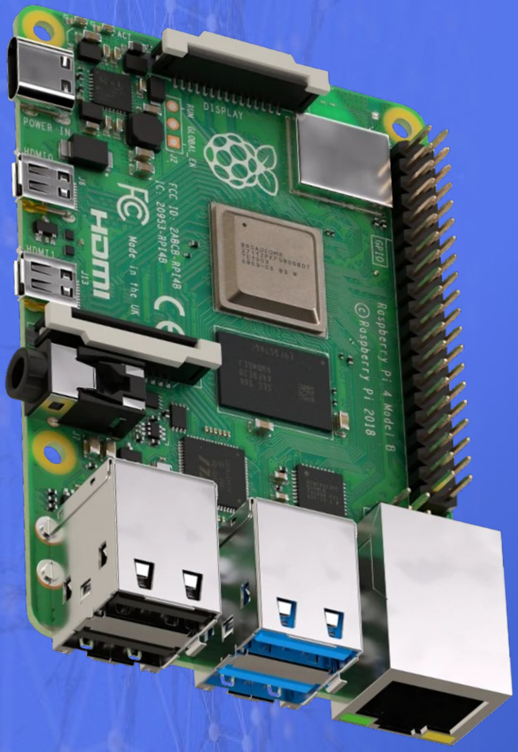
Coral & Raspberry pi 3

Si ma con prestazioni ridotte

<-USB 2.0

USB 3.0 ->

Coral & Raspberry 4

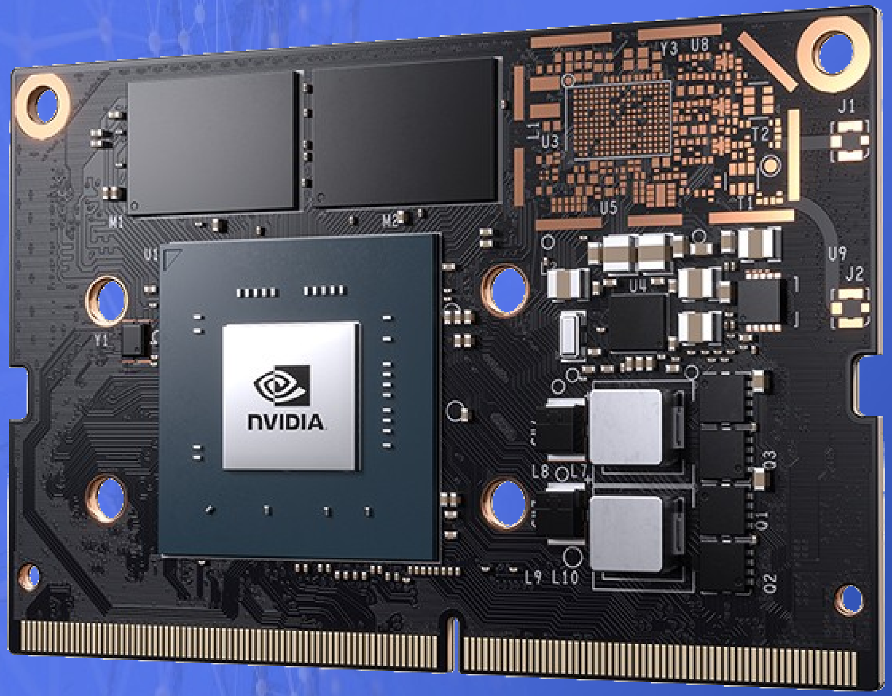


Full Match

<-USB 3.0

USB 3.0 ->

Nvidia Jetson Nano



Architettura GPU:

- NVIDIA Maxwell™ con 128 core CUDA®
- Disponibili 472 GFLOP per reti neurali
- Compatibile con PyTorch
- Compatibile con TensorFlow

Nvidia Jetson Nano

4 USB 3.0, USB 2.0 Micro-B

Connettore fotocamera CSI-2

Connettività Gigabit Ethernet, M.2 Key E

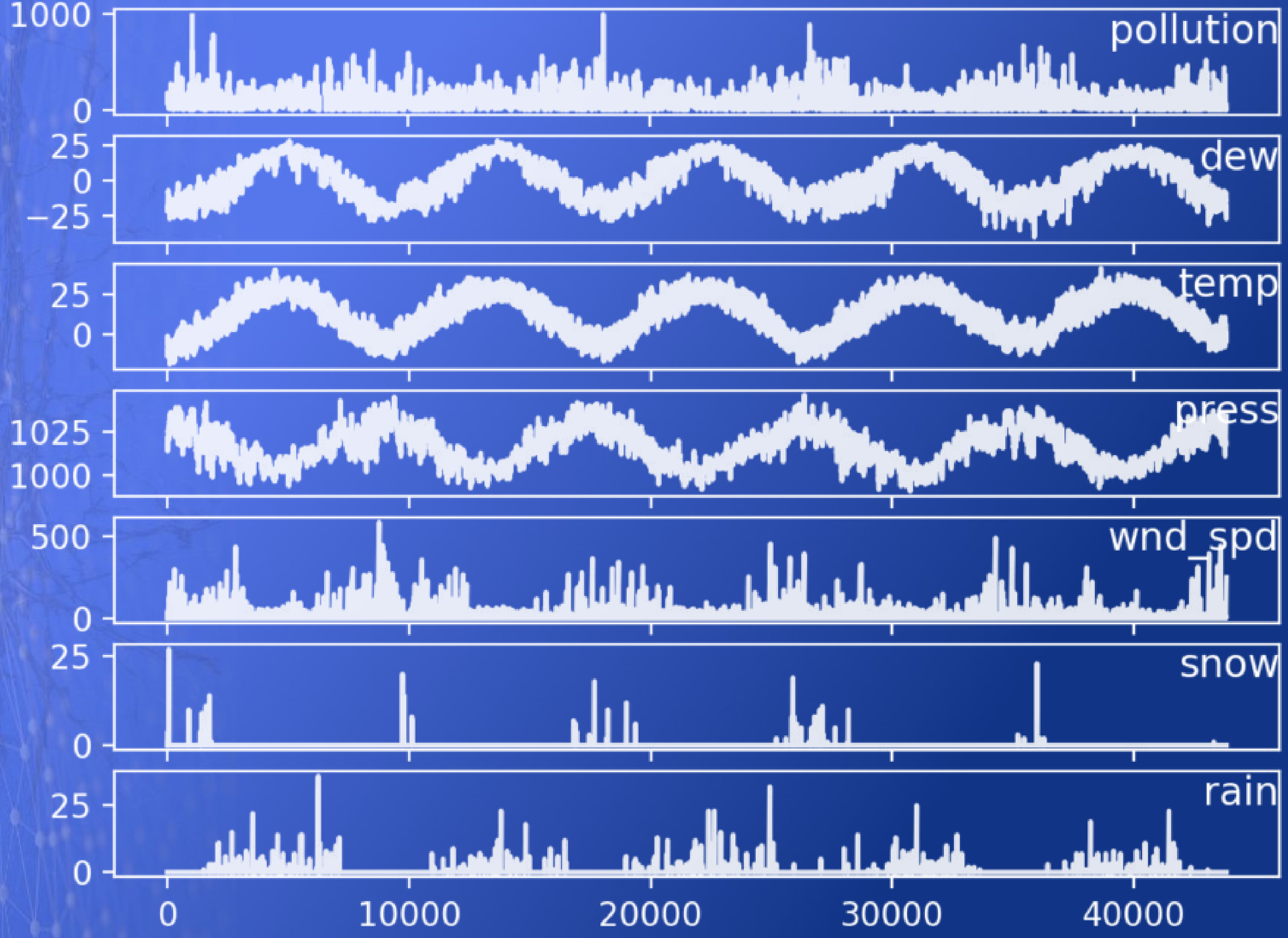
Spazio di archiviazione   microSD

Display   HDMI 2.0 e eDP 1.4

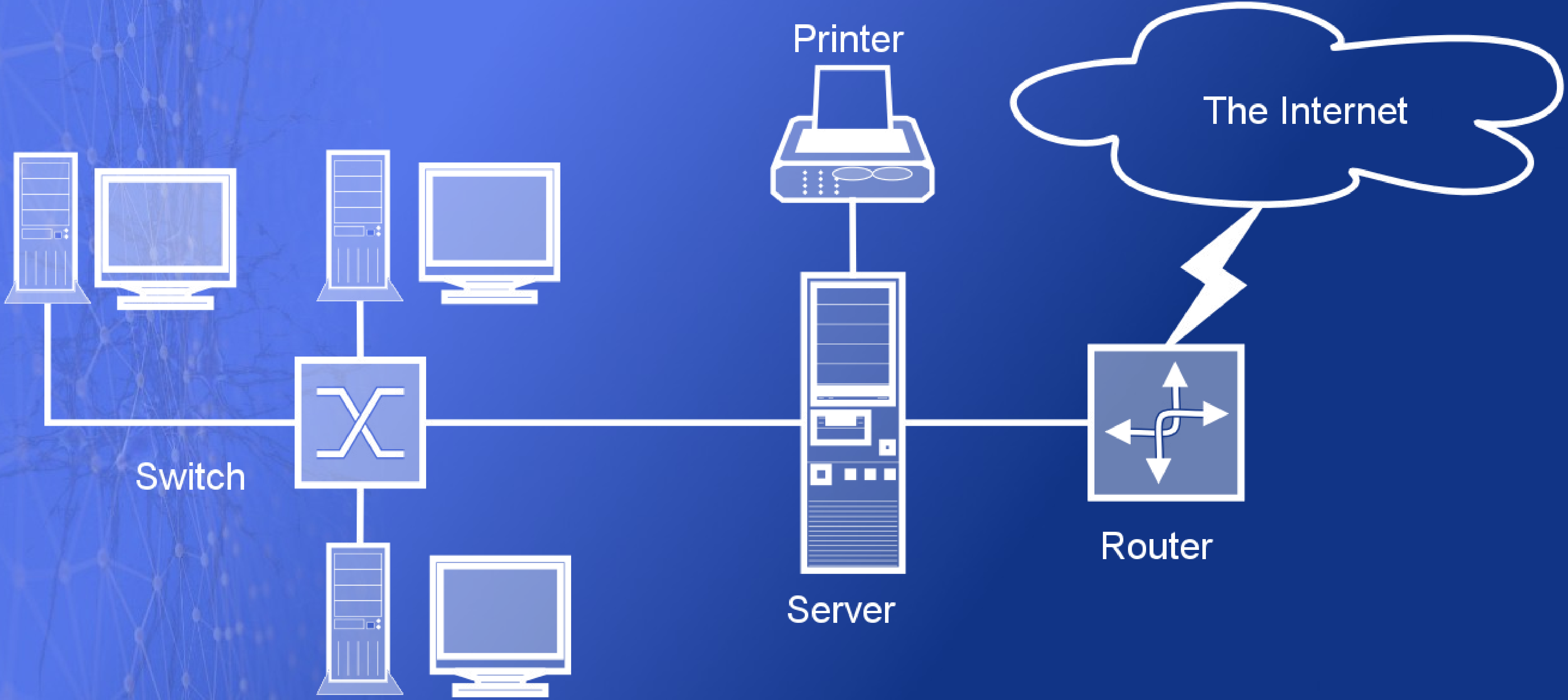
Altri GPIO, I2C, I2S, SPI, UART

Machine Learning
Osservare i dati

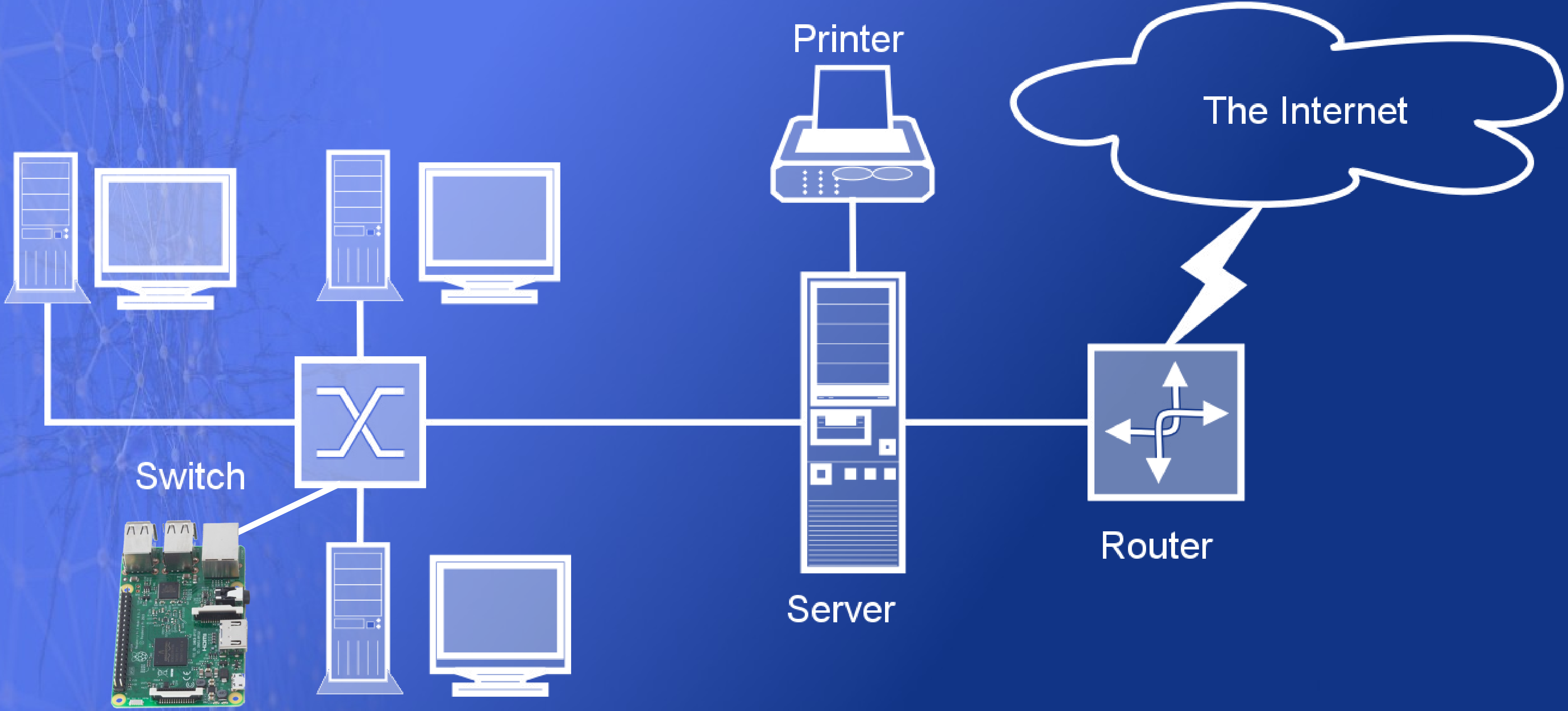
Dati nascosti nei dati



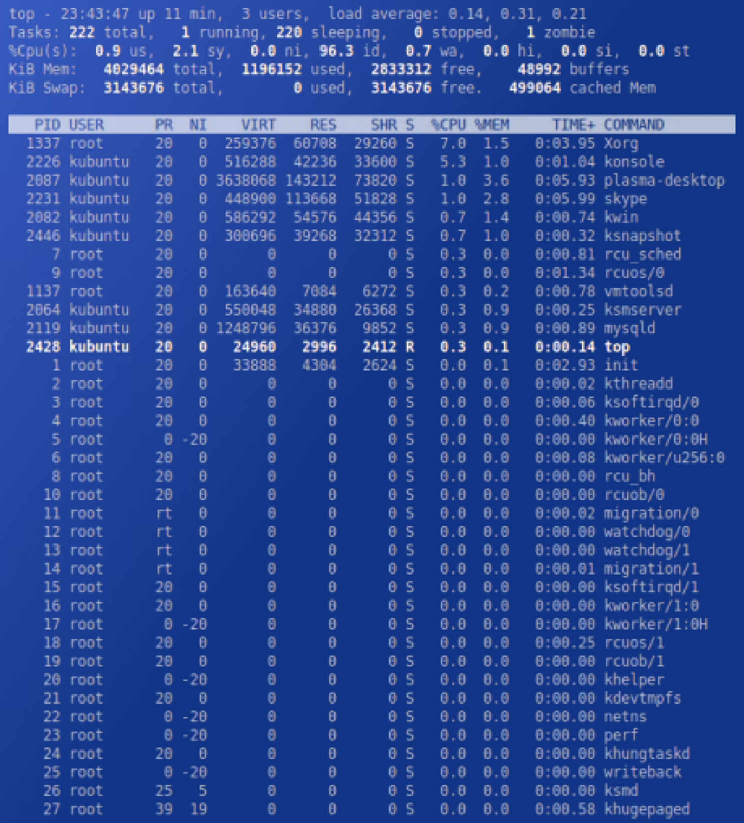
Environment



Environment



Environment to Machine Learning



```
top - 23:43:47 up 11 min,  3 users,  load average: 0.14, 0.31, 0.21
Tasks: 222 total,   1 running, 220 sleeping,   0 stopped,   1 zombie
%Cpu(s):  0.9 us,  2.1 sy,  0.0 ni, 96.3 id,  0.7 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   4029464 total,  1196152 used,  2833312 free,    48992 buffers
KiB Swap:  3143676 total,        0 used,  3143676 free.   499064 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 1337 root      20   0  259376  60708  29260 S   7.0  1.5   0:03.95 Xorg
 2226 kubuntu   20   0  516288  42236  33600 S   5.3  1.0   0:01.04 konsole
 2087 kubuntu   20   0 3638068 143212  73820 S   1.0  3.6   0:05.93 plasma-desktop
 2231 kubuntu   20   0  448900 113668  51828 S   1.0  2.8   0:05.99 skype
 2082 kubuntu   20   0  586292  54576  44356 S   0.7  1.4   0:00.74 kwin
 2446 kubuntu   20   0  300696  39268  32312 S   0.7  1.0   0:00.32 ksnapshot
    7 root      20   0       0      0      0 S   0.3  0.0   0:00.81 rcu_sched
    9 root      20   0       0      0      0 S   0.3  0.0   0:01.34 rcuos/0
 1137 root      20   0  163640   7084   6272 S   0.3  0.2   0:00.78 vmtoolsd
 2064 kubuntu   20   0  550048  34880  26368 S   0.3  0.9   0:00.25 ksmserver
 2119 kubuntu   20   0 1248796  36376   9852 S   0.3  0.9   0:00.89 mysqld
 2428 kubuntu   20   0   24960   2996   2412 R   0.3  0.1   0:00.14 top
    1 root      20   0   33888   4304   2624 S   0.0  0.1   0:02.93 init
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.02 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:00.06 ksoftirqd/0
    4 root      20   0       0      0      0 S   0.0  0.0   0:00.40 kworker/0:0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S   0.0  0.0   0:00.08 kworker/u256:0
    8 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
   10 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcuob/0
   11 root      rt   0       0      0      0 S   0.0  0.0   0:00.02 migration/0
   12 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/0
   13 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/1
   14 root      rt   0       0      0      0 S   0.0  0.0   0:00.01 migration/1
   15 root      20   0       0      0      0 S   0.0  0.0   0:00.00 ksoftirqd/1
   16 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kworker/1:0
   17 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/1:0H
   18 root      20   0       0      0      0 S   0.0  0.0   0:00.25 rcuos/1
   19 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcuob/1
   20 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 khelper
   21 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kdevtmpfs
   22 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 netns
   23 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 perf
   24 root      20   0       0      0      0 S   0.0  0.0   0:00.00 khungtaskd
   25 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 writeback
   26 root      25   5       0      0      0 S   0.0  0.0   0:00.00 ksmd
   27 root      39  19       0      0      0 S   0.0  0.0   0:00.58 khugepaged
```

Environment to Machine Learning

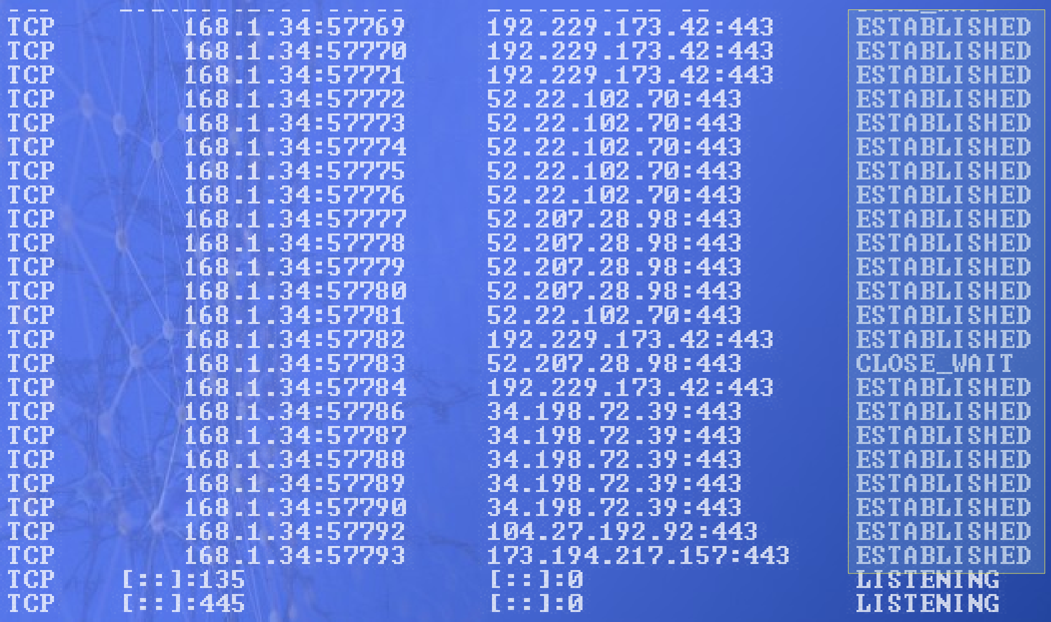
```
top - 23:43:47 up 11 min,  3 users,  load average: 0.14, 0.31, 0.21
Tasks: 222 total,   1 running, 220 sleeping,   0 stopped,   1 zombie
%Cpu(s):  0.9 us,  2.1 sy,  0.0 ni, 96.3 id,  0.7 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   4029464 total,  1196152 used,  2833312 free,    48992 buffers
KiB Swap:  3143676 total,        0 used,  3143676 free.   499064 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 1337 root      20   0  259376  60708  29260 S   7.0  1.5   0:03.95 Xorg
 2226 kubuntu   20   0  516288  42236  33600 S   5.3  1.0   0:01.04 konsole
 2087 kubuntu   20   0 3638068 143212  73820 S   1.0  3.6   0:05.93 plasma-desktop
 2231 kubuntu   20   0  448900 113668  51828 S   1.0  2.8   0:05.99 skype
 2082 kubuntu   20   0  586292  54576  44356 S   0.7  1.4   0:00.74 kwin
 2446 kubuntu   20   0  300696  39268  32312 S   0.7  1.0   0:00.32 ksnapshot
    7 root      20   0       0      0      0 S   0.3  0.0   0:00.81 rcu_sched
    9 root      20   0       0      0      0 S   0.3  0.0   0:01.34 rcuos/0
 1137 root      20   0  163640   7084   6272 S   0.3  0.2   0:00.78 vmtoolsd
 2064 kubuntu   20   0  550048  34880  26368 S   0.3  0.9   0:00.25 ksmserver
 2119 kubuntu   20   0 1248796  36376   9852 S   0.3  0.9   0:00.89 mysqld
 2428 kubuntu   20   0   24960   2996   2412 R   0.3  0.1   0:00.14 top
    1 root      20   0   33888   4304   2624 S   0.0  0.1   0:02.93 init
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.02 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:00.06 ksoftirqd/0
    4 root      20   0       0      0      0 S   0.0  0.0   0:00.40 kworker/0:0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S   0.0  0.0   0:00.08 kworker/u256:0
    8 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
   10 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcuob/0
   11 root      rt   0       0      0      0 S   0.0  0.0   0:00.02 migration/0
   12 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/0
   13 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/1
   14 root      rt   0       0      0      0 S   0.0  0.0   0:00.01 migration/1
   15 root      20   0       0      0      0 S   0.0  0.0   0:00.00 ksoftirqd/1
   16 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kworker/1:0
   17 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/1:0H
   18 root      20   0       0      0      0 S   0.0  0.0   0:00.25 rcuos/1
   19 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcuob/1
   20 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 khelper
   21 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kdevtmpfs
   22 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 netns
   23 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 perf
   24 root      20   0       0      0      0 S   0.0  0.0   0:00.00 khungtaskd
   25 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 writeback
   26 root      25   5       0      0      0 S   0.0  0.0   0:00.00 ksmd
   27 root      39  19       0      0      0 S   0.0  0.0   0:00.58 khugepaged
```

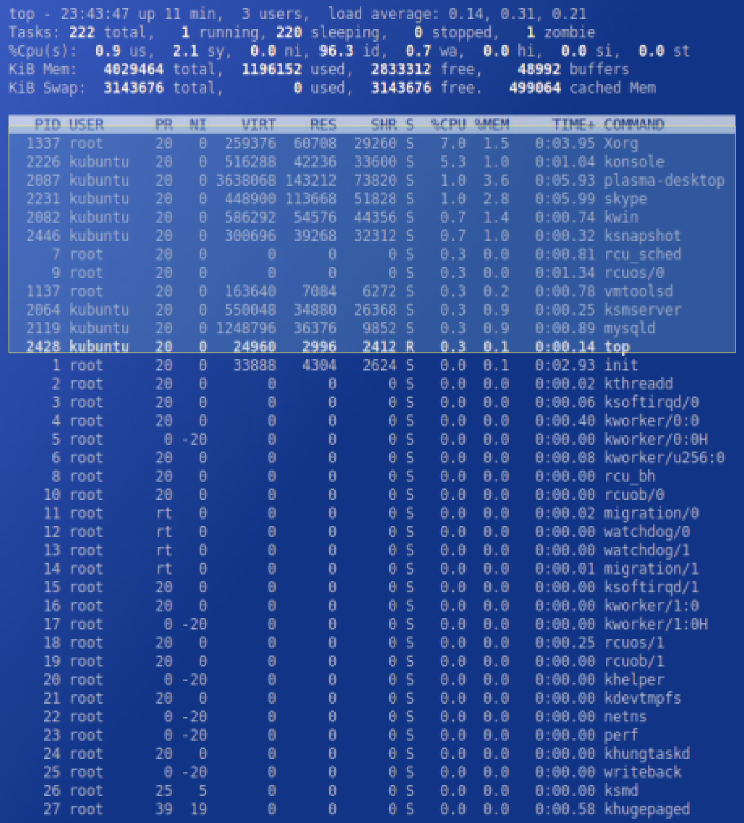
Environment to Machine Learning

```
TCP      168.1.34:57769    192.229.173.42:443    ESTABLISHED
TCP      168.1.34:57770    192.229.173.42:443    ESTABLISHED
TCP      168.1.34:57771    192.229.173.42:443    ESTABLISHED
TCP      168.1.34:57772    52.22.102.70:443      ESTABLISHED
TCP      168.1.34:57773    52.22.102.70:443      ESTABLISHED
TCP      168.1.34:57774    52.22.102.70:443      ESTABLISHED
TCP      168.1.34:57775    52.22.102.70:443      ESTABLISHED
TCP      168.1.34:57776    52.22.102.70:443      ESTABLISHED
TCP      168.1.34:57777    52.207.28.98:443      ESTABLISHED
TCP      168.1.34:57778    52.207.28.98:443      ESTABLISHED
TCP      168.1.34:57779    52.207.28.98:443      ESTABLISHED
TCP      168.1.34:57780    52.207.28.98:443      ESTABLISHED
TCP      168.1.34:57781    52.22.102.70:443      ESTABLISHED
TCP      168.1.34:57782    192.229.173.42:443    ESTABLISHED
TCP      168.1.34:57783    52.207.28.98:443      CLOSE_WAIT
TCP      168.1.34:57784    192.229.173.42:443    ESTABLISHED
TCP      168.1.34:57786    34.198.72.39:443      ESTABLISHED
TCP      168.1.34:57787    34.198.72.39:443      ESTABLISHED
TCP      168.1.34:57788    34.198.72.39:443      ESTABLISHED
TCP      168.1.34:57789    34.198.72.39:443      ESTABLISHED
TCP      168.1.34:57790    34.198.72.39:443      ESTABLISHED
TCP      168.1.34:57792    104.27.192.92:443     ESTABLISHED
TCP      168.1.34:57793    173.194.217.157:443   ESTABLISHED
TCP    [::]:135            [::]:0                LISTENING
TCP    [::]:445            [::]:0                LISTENING
```

```
top - 23:43:47 up 11 min,  3 users,  load average: 0.14, 0.31, 0.21
Tasks: 222 total,   1 running, 220 sleeping,   0 stopped,   1 zombie
%Cpu(s):  0.9 us,  2.1 sy,  0.0 ni, 96.3 id,  0.7 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem:   4029464 total,  1196152 used,  2833312 free,    48992 buffers
KiB Swap:  3143676 total,        0 used,  3143676 free.   499064 cached Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 1337 root      20   0  259376  60708  29260 S   7.0  1.5   0:03.95 Xorg
 2226 kubuntu   20   0  516288  42236  33600 S   5.3  1.0   0:01.04 konsole
 2087 kubuntu   20   0 3638068 143212  73820 S   1.0  3.6   0:05.93 plasma-desktop
 2231 kubuntu   20   0  448900 113668  51828 S   1.0  2.8   0:05.99 skype
 2082 kubuntu   20   0  586292  54576  44356 S   0.7  1.4   0:00.74 kwin
 2446 kubuntu   20   0  300696  39268  32312 S   0.7  1.0   0:00.32 ksnapshot
    7 root      20   0       0      0      0 S   0.3  0.0   0:00.81 rcu_sched
    9 root      20   0       0      0      0 S   0.3  0.0   0:01.34 rcuos/0
 1137 root      20   0  163640   7084   6272 S   0.3  0.2   0:00.78 vmtoolsd
 2064 kubuntu   20   0  550048  34880  26368 S   0.3  0.9   0:00.25 ksmserver
 2119 kubuntu   20   0 1248796  36376   9852 S   0.3  0.9   0:00.89 mysqld
 2428 kubuntu   20   0   24960   2996   2412 R   0.3  0.1   0:00.14 top
    1 root      20   0   33888   4304   2624 S   0.0  0.1   0:02.93 init
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.02 kthreadd
    3 root      20   0       0      0      0 S   0.0  0.0   0:00.06 ksoftirqd/0
    4 root      20   0       0      0      0 S   0.0  0.0   0:00.40 kworker/0:0
    5 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    6 root      20   0       0      0      0 S   0.0  0.0   0:00.08 kworker/u256:0
    8 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
   10 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcuob/0
   11 root      rt   0       0      0      0 S   0.0  0.0   0:00.02 migration/0
   12 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/0
   13 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 watchdog/1
   14 root      rt   0       0      0      0 S   0.0  0.0   0:00.01 migration/1
   15 root      20   0       0      0      0 S   0.0  0.0   0:00.00 ksoftirqd/1
   16 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kworker/1:0
   17 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/1:0H
   18 root      20   0       0      0      0 S   0.0  0.0   0:00.25 rcuos/1
   19 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcuob/1
   20 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 khelper
   21 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kdevtmpfs
   22 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 netns
   23 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 perf
   24 root      20   0       0      0      0 S   0.0  0.0   0:00.00 khungtaskd
   25 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 writeback
   26 root      25   5       0      0      0 S   0.0  0.0   0:00.00 ksmd
   27 root      39  19       0      0      0 S   0.0  0.0   0:00.58 khugepaged
```

Environment to Machine Learning





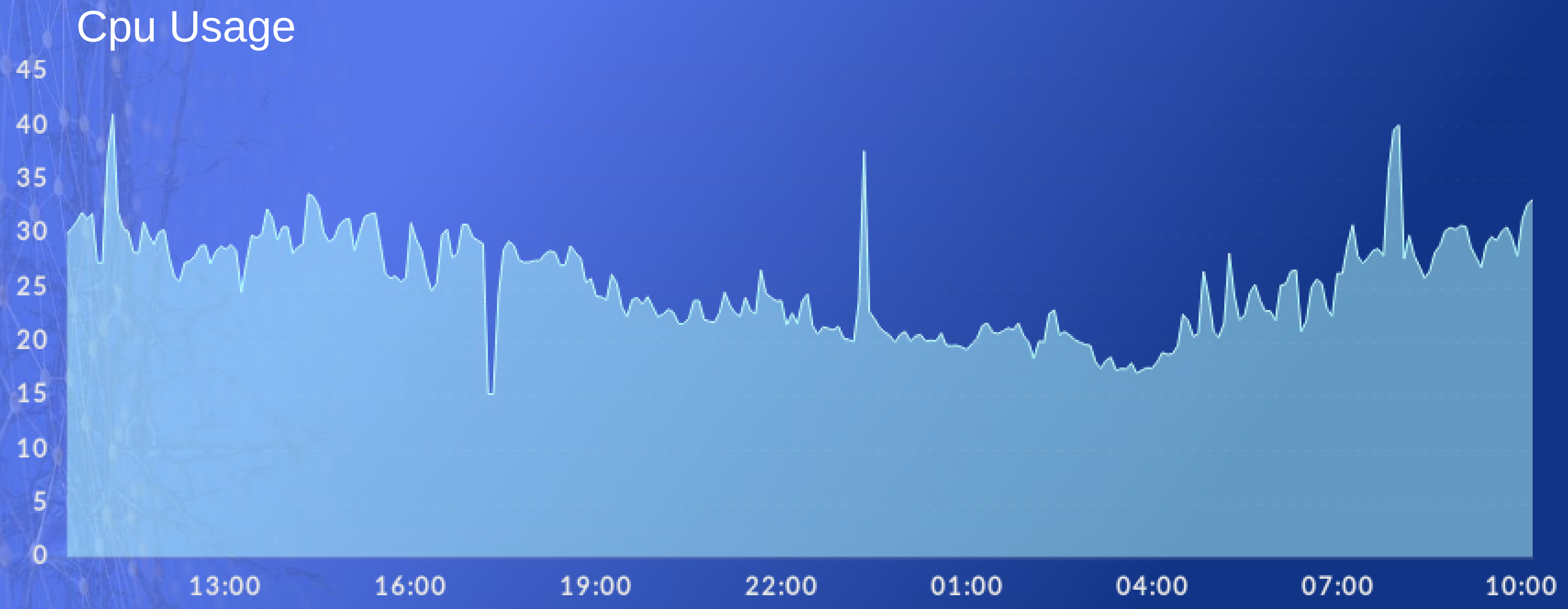
Environment to Machine Learning

```
              12.5Kb          25.0Kb          37.5Kb          50.0Kb     62.5Kb

dev-machine-2.local:44467  => 202.146.4.100:http         5.80Kb  1.16Kb   297b
                           <=                             102Kb  20.3Kb  5.08Kb
dev-machine-2.local:59566  => 202.146.4.17:http           208b   1.18Kb   301b
                           <=                             208b   17.6Kb  4.40Kb
dev-machine-2.local:40258  => 202.146.4.2:http           10.7Kb  2.22Kb   568b
                           <=                            74.1Kb  14.9Kb  3.72Kb
dev-machine-2.local:40255  => 202.146.4.2:http           9.92Kb  2.07Kb   530b
                           <=                            59.4Kb  11.9Kb  2.98Kb
dev-machine-2.local:40256  => 202.146.4.2:http           8.05Kb  1.70Kb   435b
                           <=                            55.8Kb  11.2Kb  2.80Kb
dev-machine-2.local:40261  => 202.146.4.2:http           10.1Kb  2.02Kb   517b
                           <=                            49.9Kb  9.98Kb  2.49Kb
dev-machine-2.local:40257  => 202.146.4.2:http           11.5Kb  2.39Kb   611b
                           <=                            37.6Kb  7.56Kb  1.89Kb
dev-machine-2.local:40259  => 202.146.4.2:http           10.7Kb  2.23Kb   570b
                           <=                            18.2Kb  3.68Kb   943b
dev-machine-2.local:33464  => kul06s06-in-f16.1e10:https     0b  1.66Kb   424b
                           <=                                0b  4.08Kb  1.02Kb

TX:             cumm:  32.5KB   peak:   83.4Kb  rates:   83.4Kb  24.5Kb  6.19Kb
RX:                     156KB            435Kb            435Kb   124Kb  31.0Kb
TOTAL:                  189KB            519Kb            519Kb   148Kb  37.2Kb
```

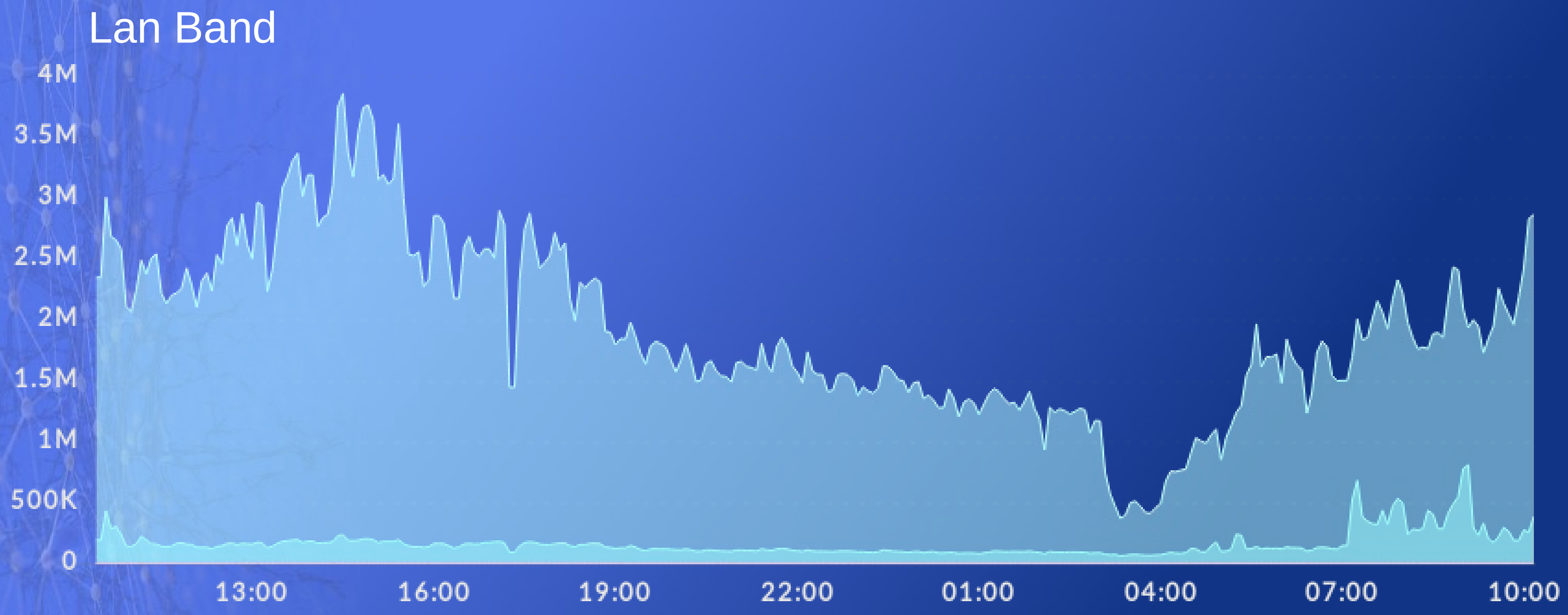
Environment to Machine Learning

```
              12.5Kb          25.0Kb          37.5Kb          50.0Kb     62.5Kb

dev-machine-2.local:44467  => 202.146.4.100:http        5.80Kb  1.16Kb   297b
                           <=                           102Kb  20.3Kb  5.08Kb
dev-machine-2.local:59566  => 202.146.4.17:http          208b  1.18Kb   301b
                           <=                            208b  17.6Kb  4.40Kb
dev-machine-2.local:40258  => 202.146.4.2:http          10.7Kb  2.22Kb   568b
                           <=                           74.1Kb  14.9Kb  3.72Kb
dev-machine-2.local:40255  => 202.146.4.2:http          9.92Kb  2.07Kb   530b
                           <=                           59.4Kb  11.9Kb  2.98Kb
dev-machine-2.local:40256  => 202.146.4.2:http          8.05Kb  1.70Kb   435b
                           <=                           55.8Kb  11.2Kb  2.80Kb
dev-machine-2.local:40261  => 202.146.4.2:http          10.1Kb  2.02Kb   517b
                           <=                           49.9Kb  9.98Kb  2.49Kb
dev-machine-2.local:40257  => 202.146.4.2:http          11.5Kb  2.39Kb   611b
                           <=                           37.6Kb  7.56Kb  1.89Kb
dev-machine-2.local:40259  => 202.146.4.2:http          10.7Kb  2.23Kb   570b
                           <=                           18.2Kb  3.68Kb   943b
dev-machine-2.local:33464  => kul06s06-in-f16.1e10:https    0b  1.66Kb   424b
                           <=                               0b  4.08Kb  1.02Kb

TX:              cumm:  32.5KB   peak:   83.4Kb  rates:   83.4Kb  24.5Kb  6.19Kb
RX:                     156KB            435Kb            435Kb   124Kb   31.0Kb
TOTAL:                  189KB            519Kb            519Kb   148Kb   37.2Kb
```

Environment to Machine Learning

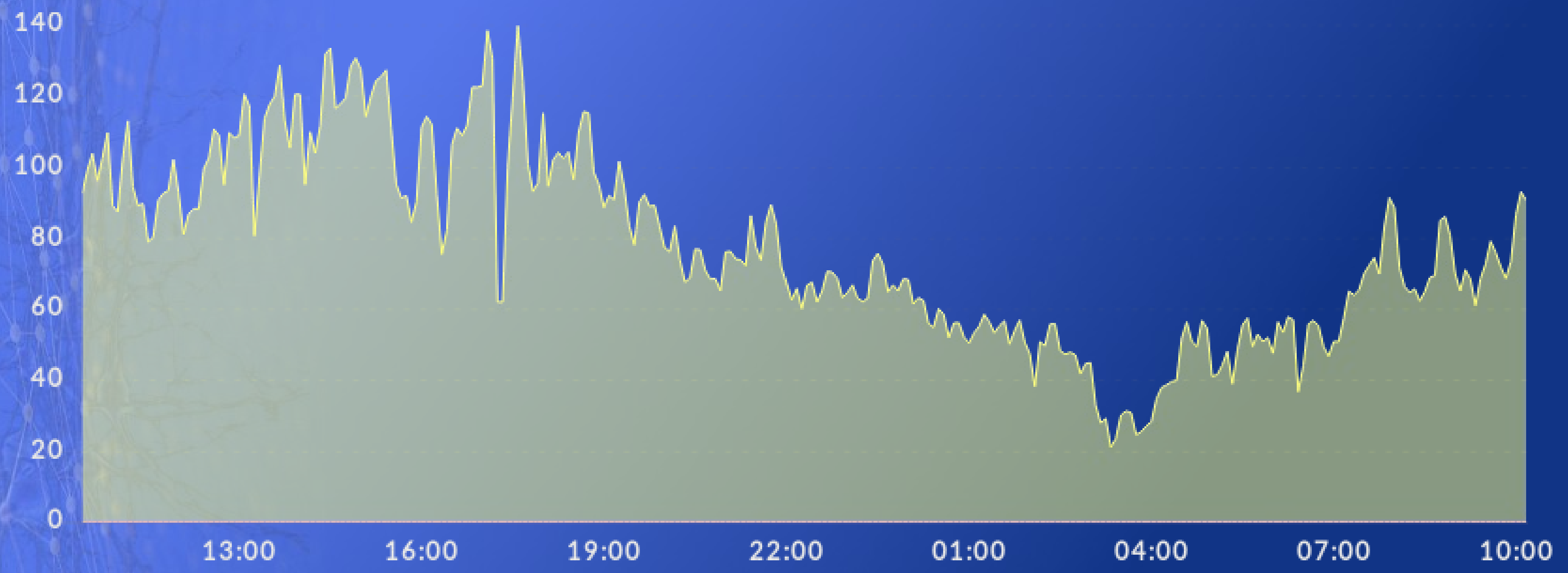


Environment to Machine Learning



Environment to Machine Learning

Disk I/O



Environment to Machine Learning

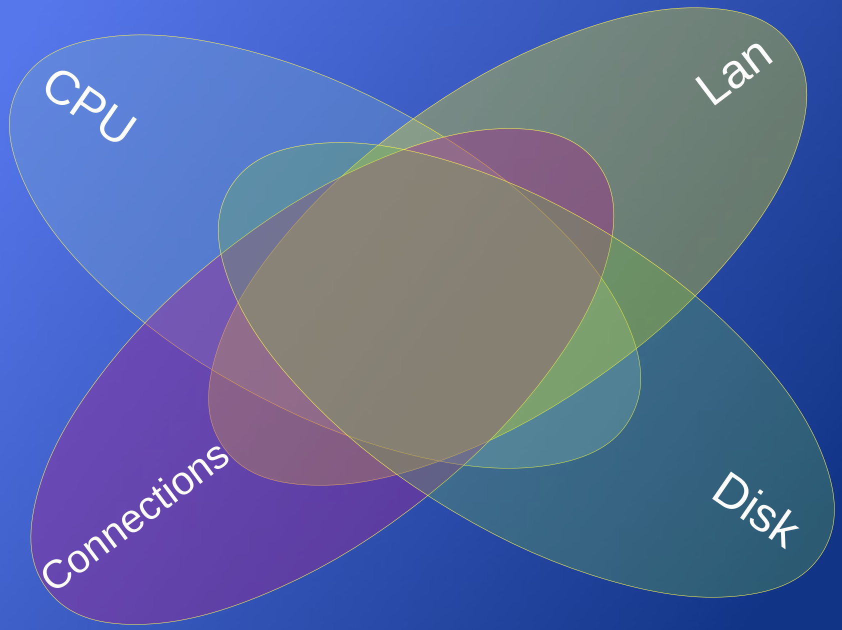
Cpu Usage

Lan Band

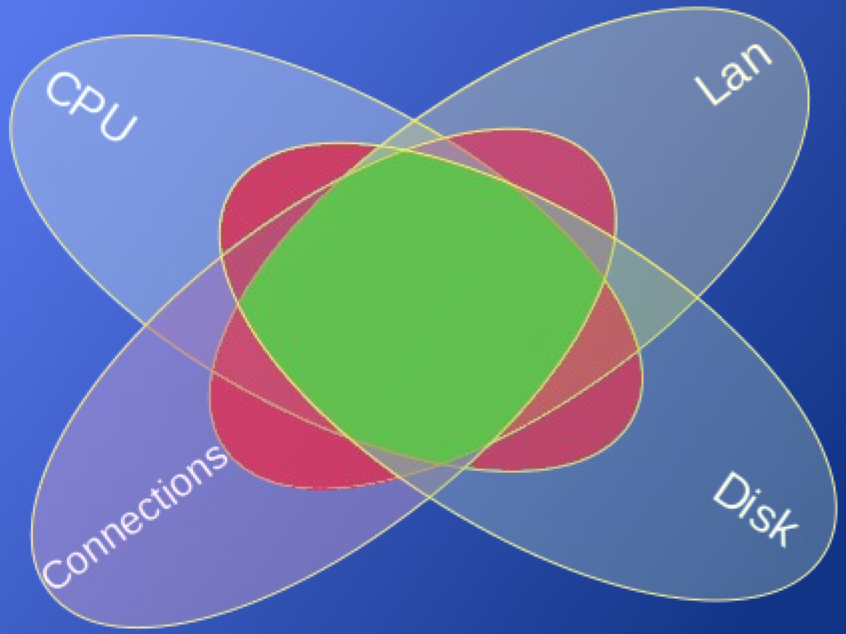
Disk I/O

Total Connections

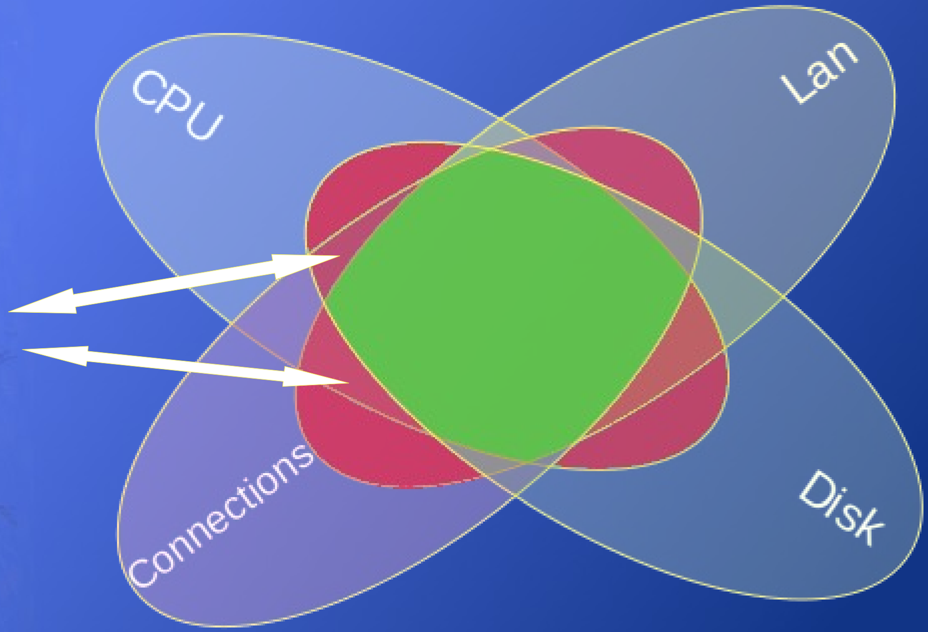
Environment to Machine Learning



Environment to Machine Learning

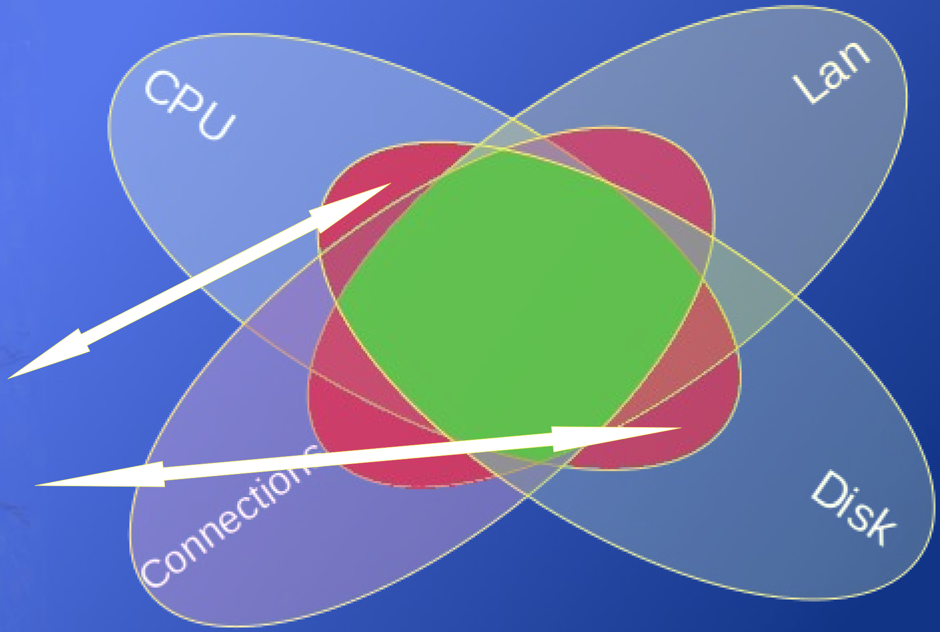


Environment to Machine Learning



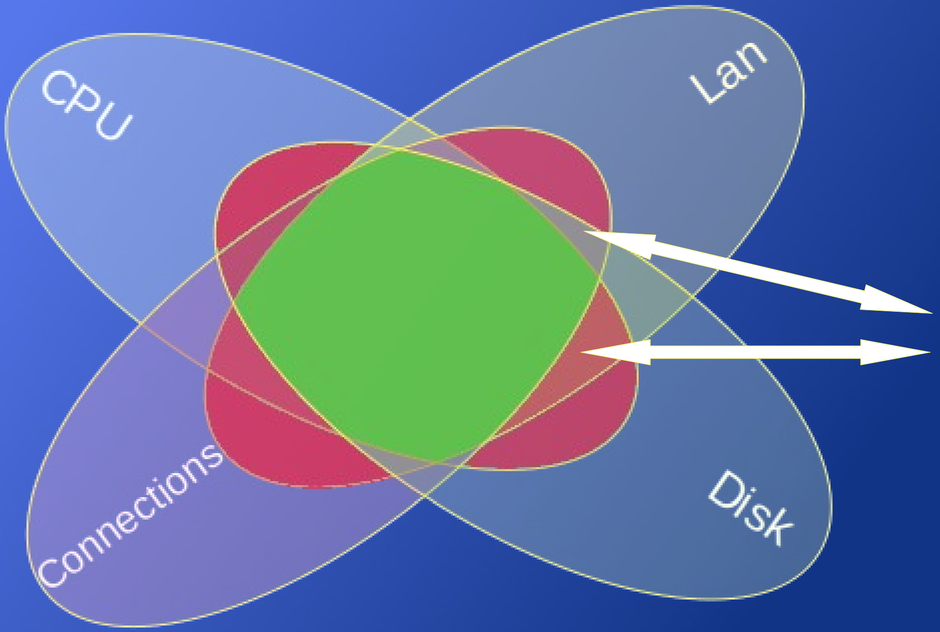
CPU + Connections
Denial Of Service

Environment to Machine Learning



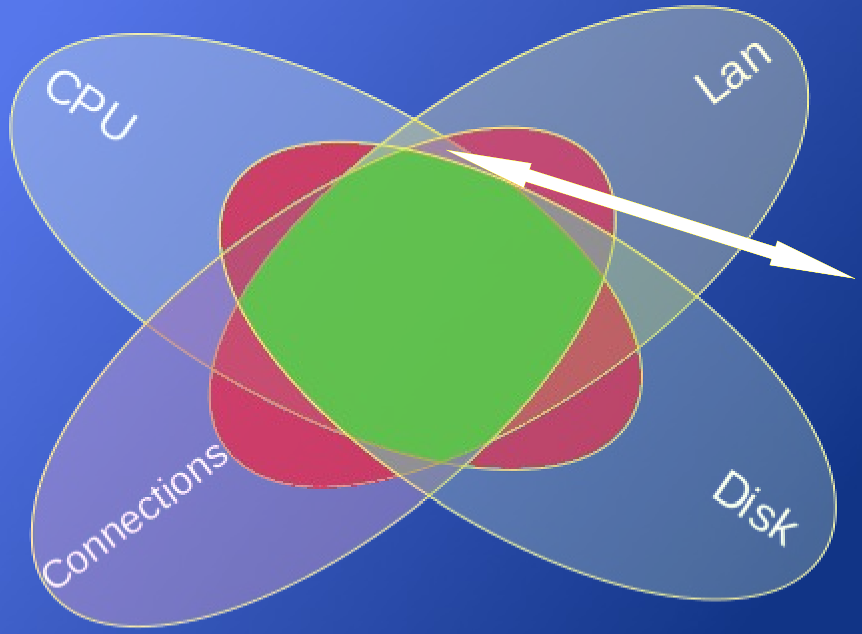
CPU + Disk
RamsonWare

Environment to Machine Learning



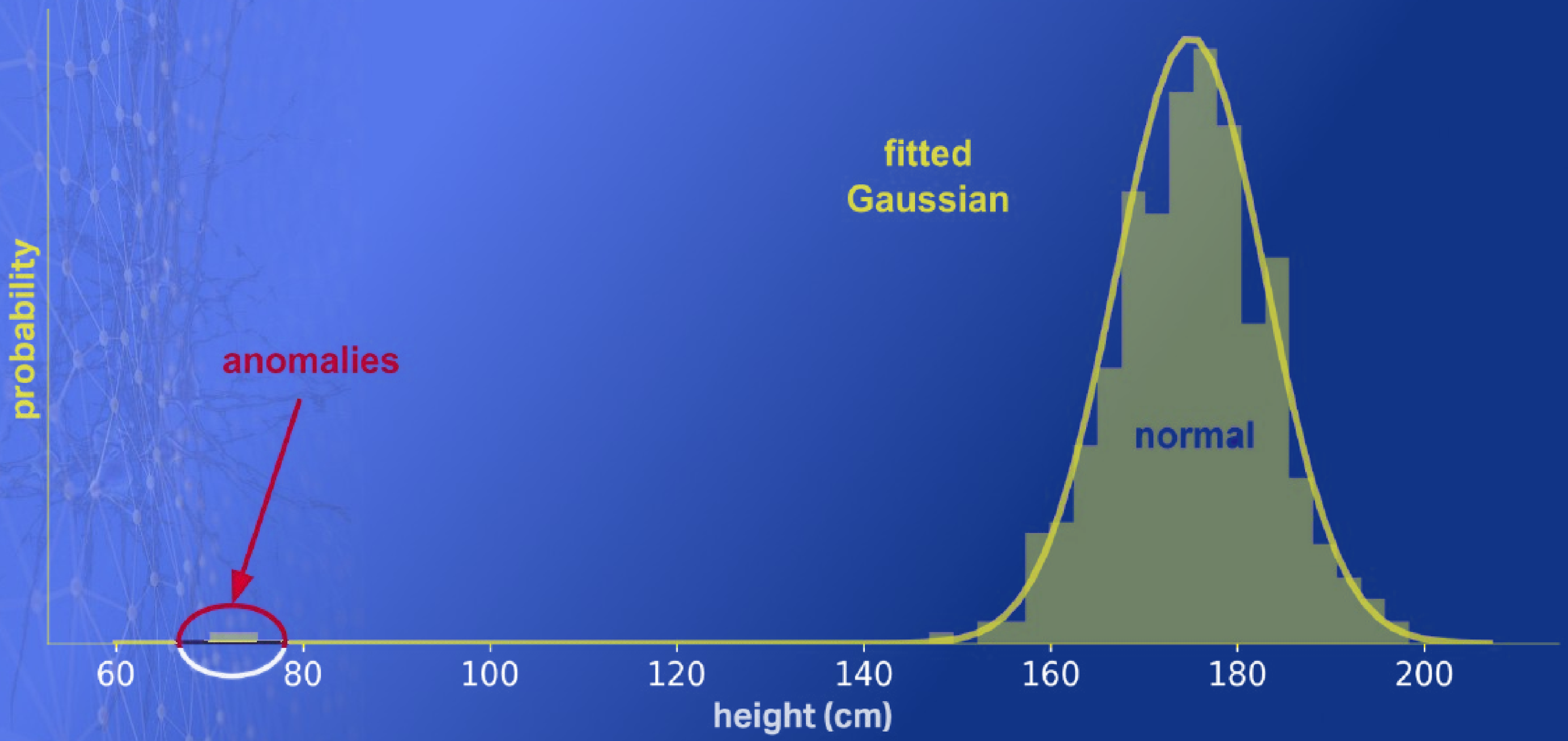
Disk + Lan
Malware
Data Stolen

Environment to Machine Learning



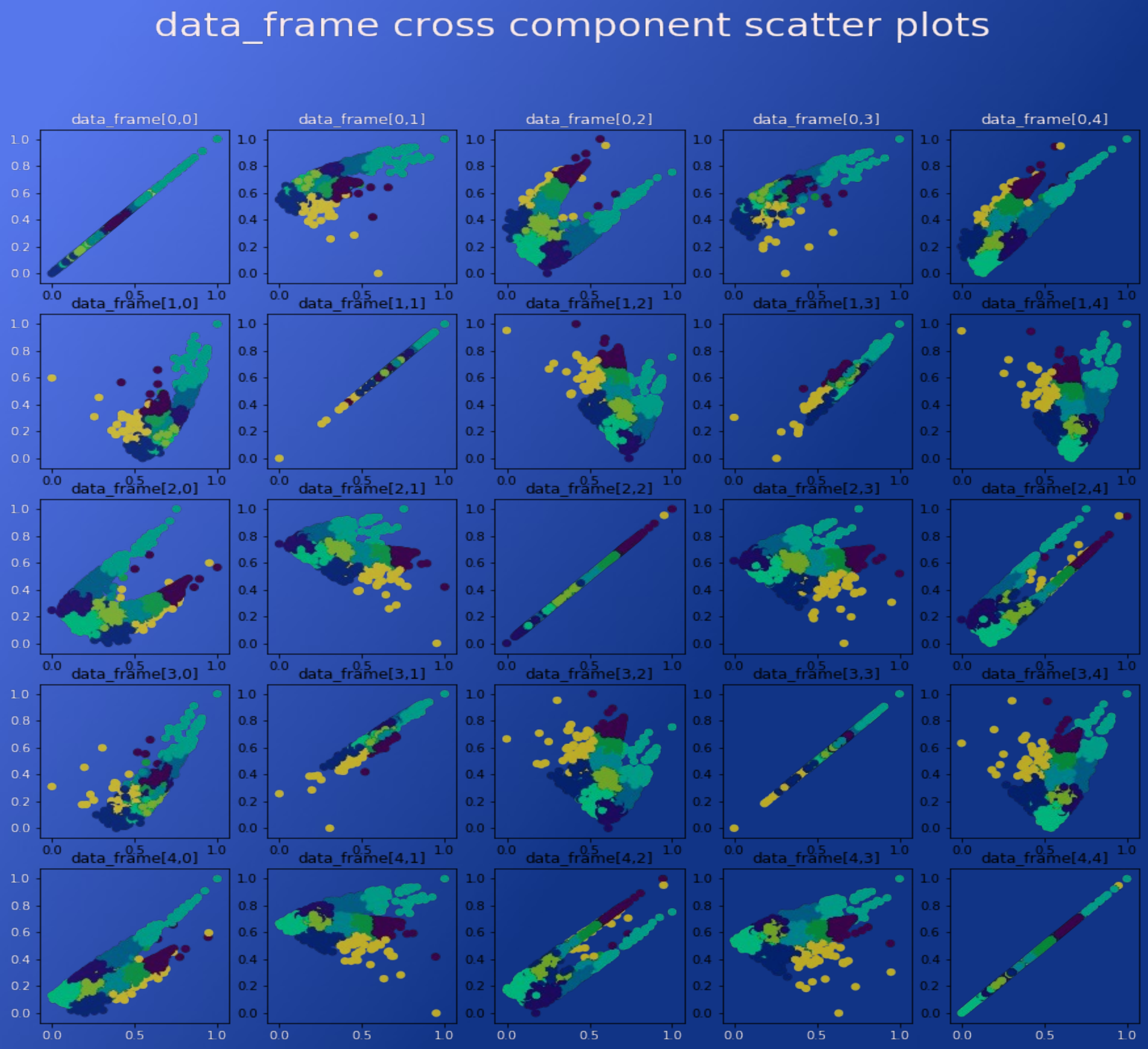
CPU + Lan
Malware
Activity Monitoring

Anomaly Detection



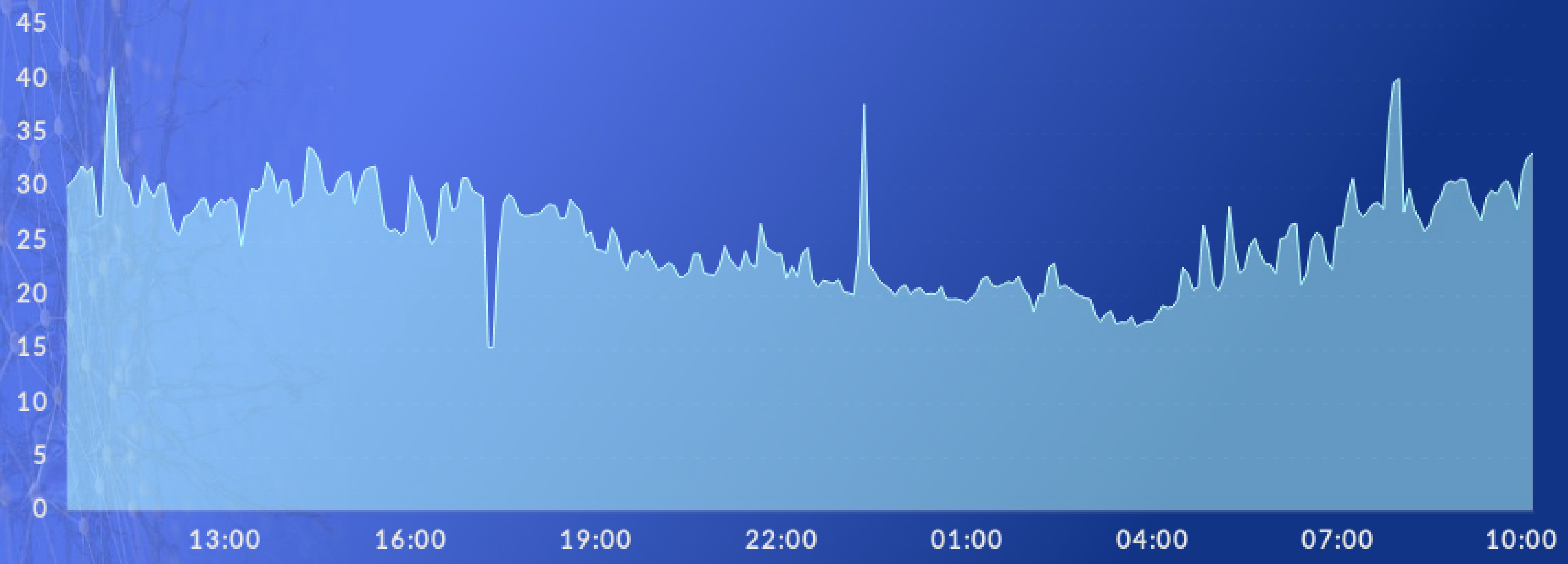
Anomaly Detection

Multi-dimentional Problems

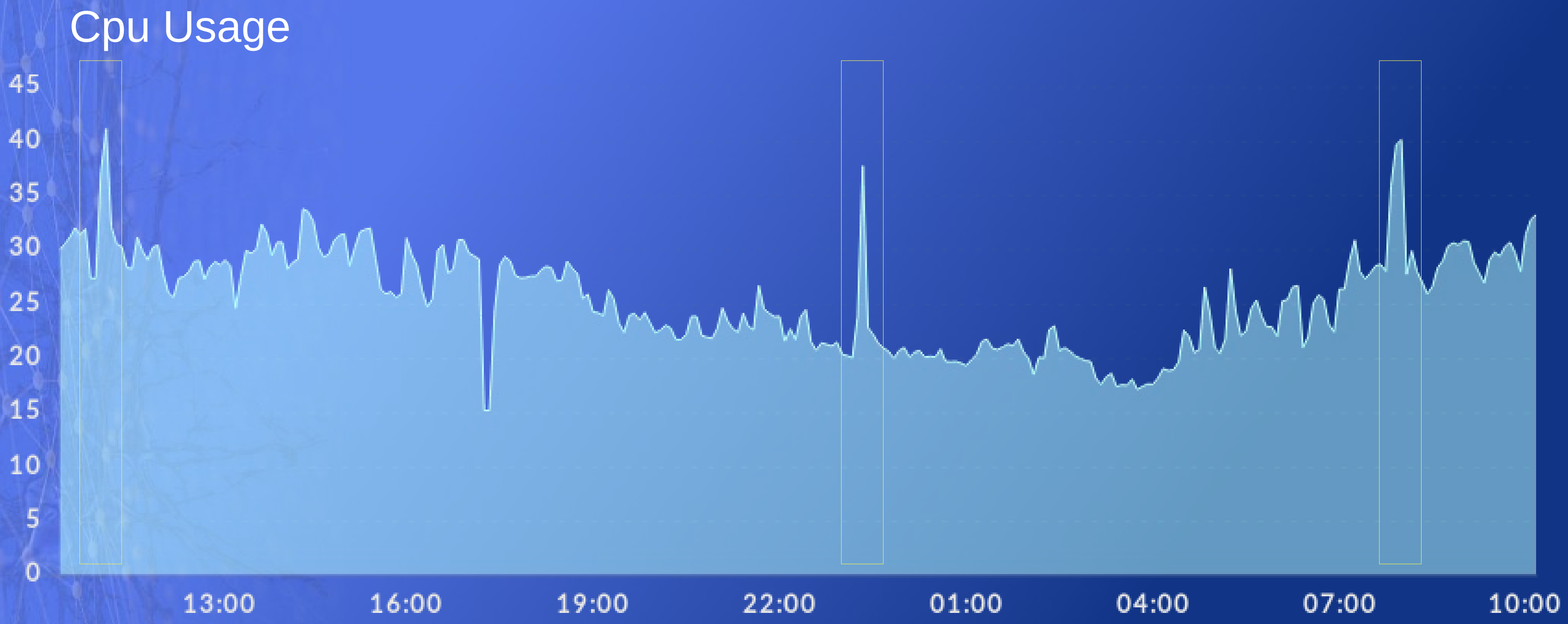


Environment to Machine Learning

Cpu Usage



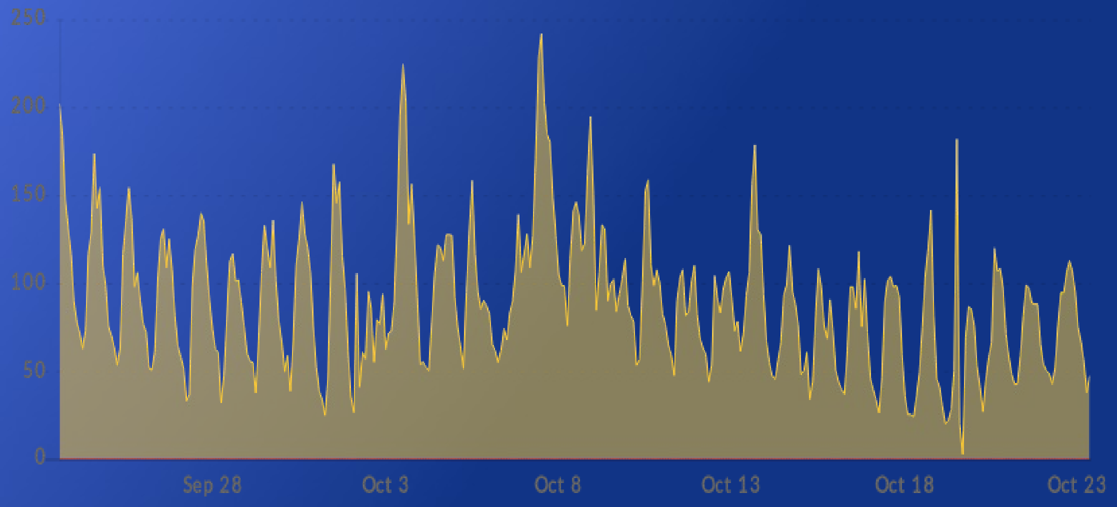
Environment to Machine Learning



Time Series (Serie Storiche)

Interpretare un fenomeno che si sviluppa nel tempo:

- Trend
- Ciclicità
- Stagionalità
- Accidentalità
- previsioni di andamento futuro



Serie Storiche Multivariate

Le variabili delle serie storiche non dipendono solo da se stesse (Autocorrelate)
ma spesso dipendo anche da altre variabili (Cross-Correlate)

Queste relazioni multiple vanno considerate al fine di migliorare le capacità predittive

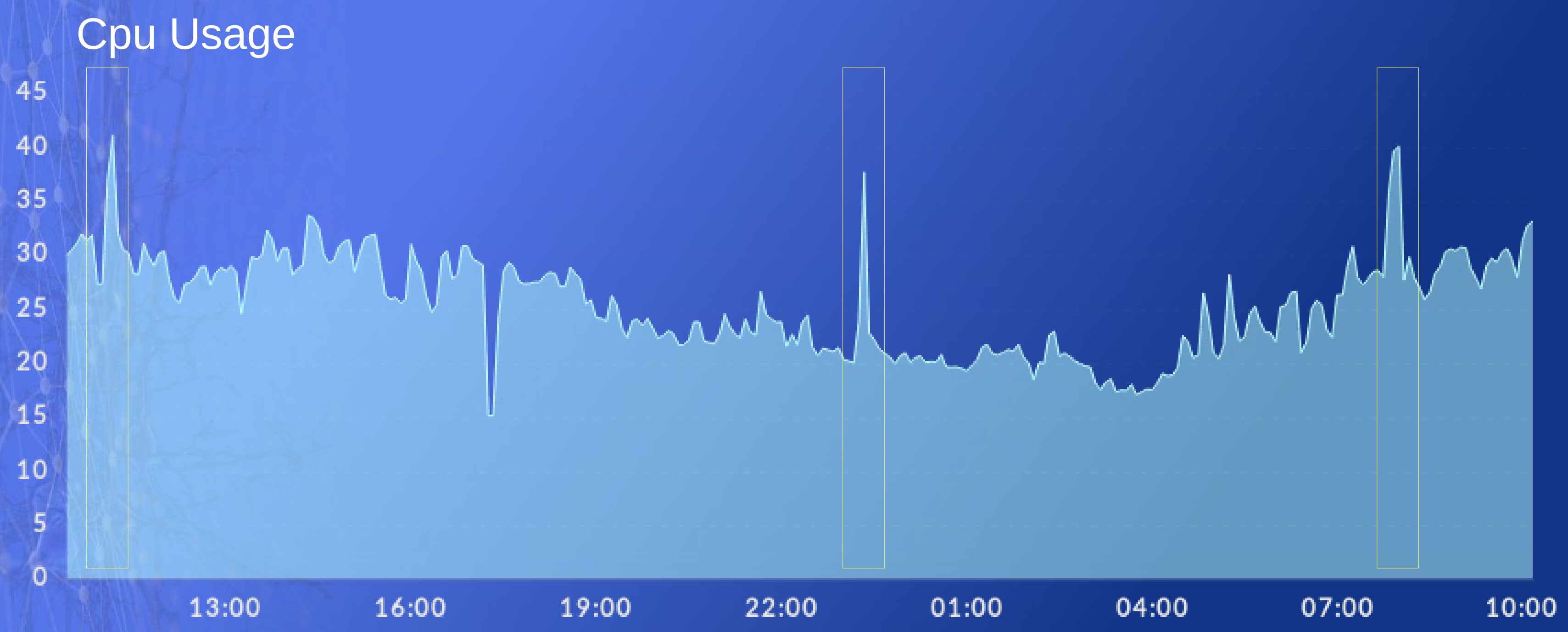
Tuttavia questo aumenta enormemente le capacità di calcolo necessarie

Nel caso del raspberry l’utilizzo degli algoritmi delle Time-Series potrebbe non essere la scelta migliore

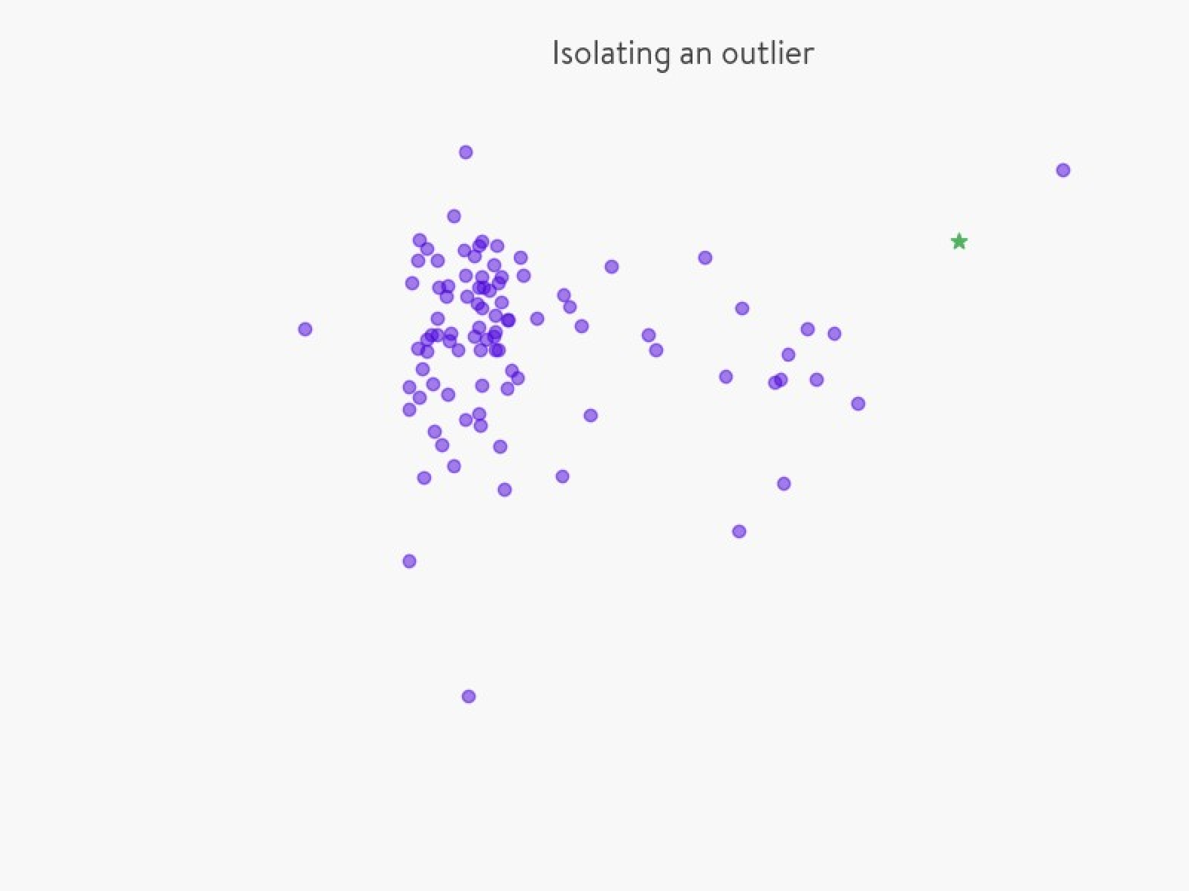
Quale alternativa potrebbe funzionare?

Isolation Forest

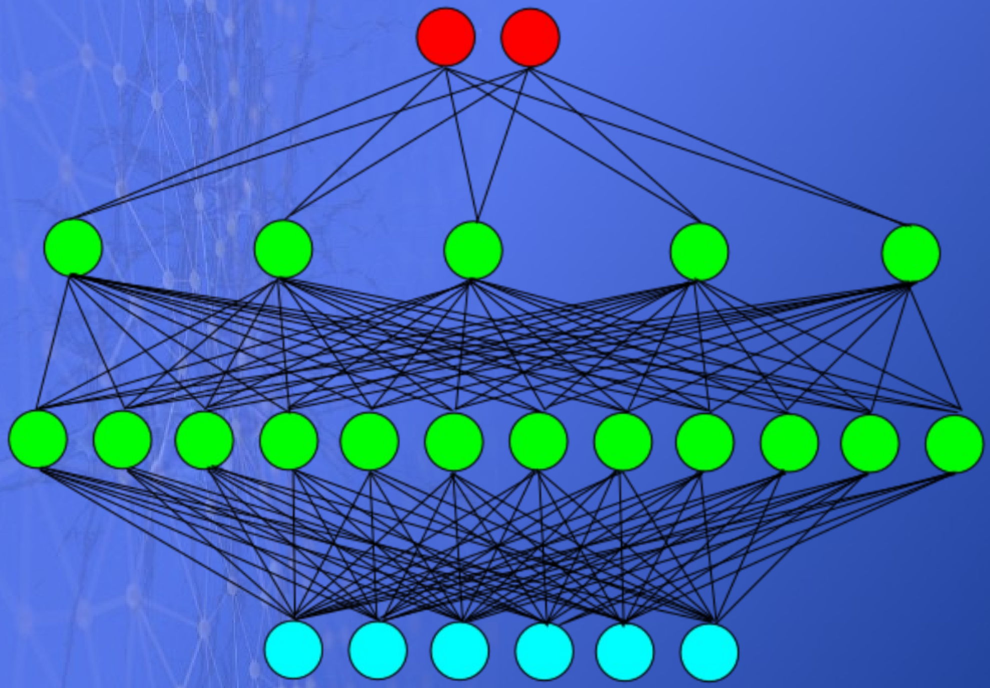
Isolation Forest

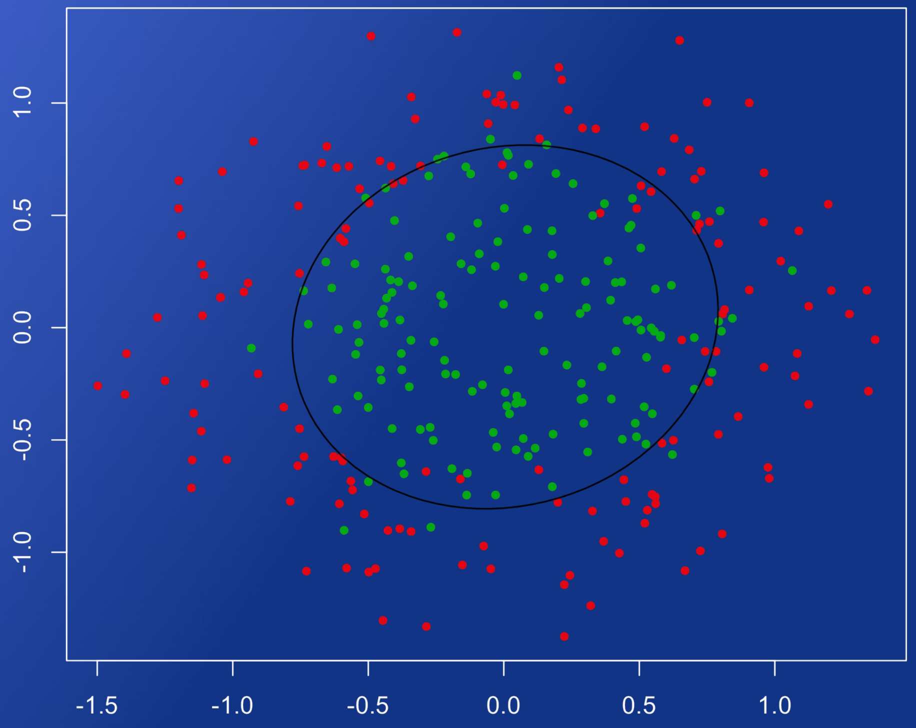


Isolation Forest



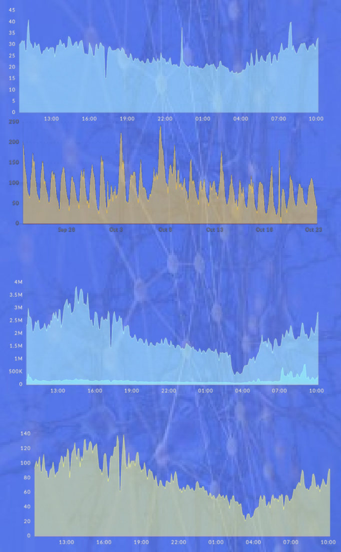
Classificazione degli eventi

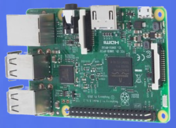




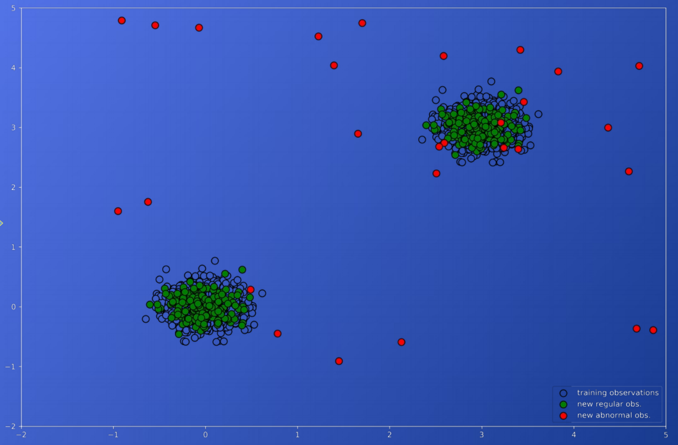
Schema complessivo del Rilevatore

Sampling

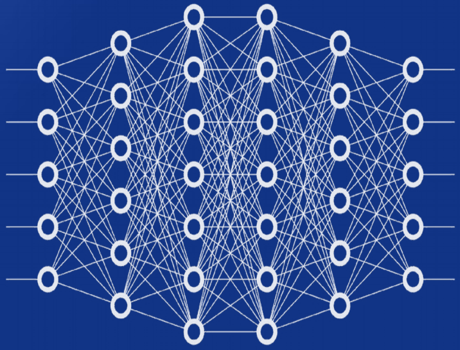




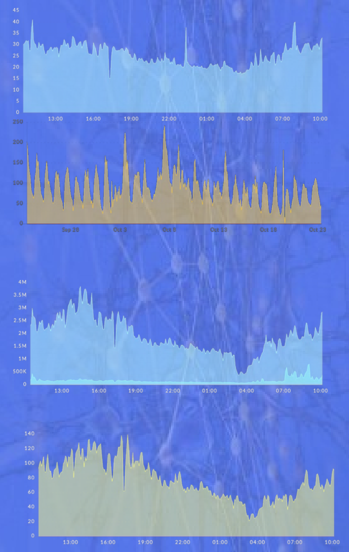
Outlier Detection

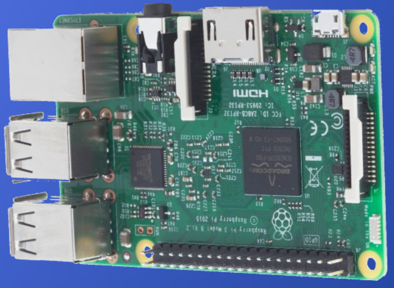


Classification



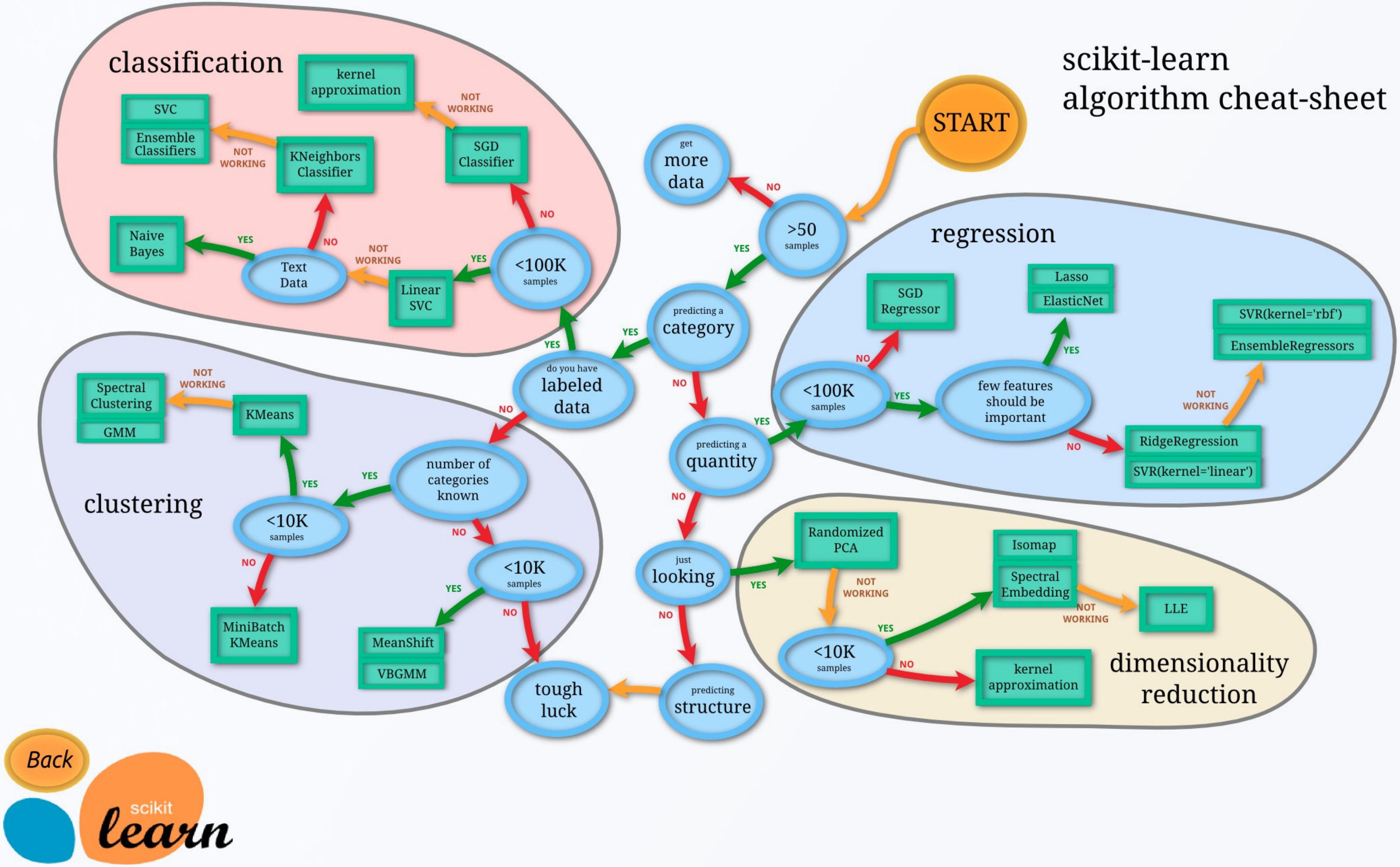
Schema complessivo del Rilevatore





Riferimenti Software suggeriti per Raspberry

- Numpy per il calcolo matriciale e metriche
- Sklearn per implementazione Isolation Forest
- Sklearn per implementazione Classificatore


scikit-learn
algorithm cheat-sheet
START
>50 samples
get more data
predicting a category
do you have labeled data
<100K samples
SGD Classifier
kernel approximation
Linear SVC
Text Data
Naive Bayes
KNeighbors Classifier
SVC
Ensemble Classifiers
classification
number of categories known
<10K samples
KMeans
Spectral Clustering
GMM
MiniBatch KMeans
<10K samples
MeanShift
VBGMM
clustering
tough luck
predicting a quantity
regression
<100K samples
SGD Regressor
few features should be important
Lasso
ElasticNet
RidgeRegression
SVR(kernel='linear')
SVR(kernel='rbf')
EnsembleRegressors
just looking
predicting structure
Randomized PCA
<10K samples
Isomap
Spectral Embedding
LLE
kernel approximation
dimensionality reduction
YES
NO
NOT WORKING
Back
scikit learn

Come contattarmi

@: annino.nicolo@gmail.com

in nicolo-annino

Riferimenti per Machine Learning

Machine Learning Italia

iaml
ITALIAN ASSOCIATION FOR MACHINE LEARNING

“Il confine tra realtà e fantasia giace sul palmo della mano”

Grazie per l’ascolto

IDEALARM®